Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

o0o

DAMIAN FLORES

Plaintiff,

v.

EQUIFAX, INC.,

Defendant.

Case No.: 1:18-CV-0117

VERIFIED COMPLAINT FOR DAMAGES

(JURY TRIAL REQUESTED)

NATURE OF CASE

1. Plaintiff brings this case against Defendant Equifax for its gargantuan failures to secure and safeguard Plaintiff's personal identifiable information ("PII"), which Equifax collected from various sources in connection with the operation of its business as a consumer credit reporting agency, and for failing to provide timely, accurate and adequate notice to Consumers such as Plaintiff.

2. Equifax has acknowledged that a cybersecurity incident ("Data Breach") potentially impacting approximately 143 million U.S. consumers. It has also acknowledged that unauthorized persons exploited a U.S. website application vulnerability to gain access to certain files. Equifax claims that based on its investigation, the unauthorized access occurred from mid-May through July 2017. The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, Equifax has admitted that credit card numbers for approximately 209,000 U.S. consumers, and certain dispute

documents with personal identifying information for approximately 182, 000 U.S. consumers, was accessed and stolen by hackers and sold on the dark web. All due to Defendants inadequate security systems.

3. Equifax has acknowledged that it discovered the unauthorized access on July 29, 2017, but has failed to inform the public why it delayed notification of the Data Breach to consumers. Instead, Equifax executives sold at least $1.8 million worth of shares before the public disclosure of the breach. It has been reported that its Chief Financial Officer John Gamble sold shares worth $946,374, its president of U.S. information solutions, Joseph Loughran, exercised options to dispose of stock worth $584,099, and its president of workforce solutions, Rodolfo Ploder sold $250,458 of stock on August 2, 2017.

4. The PII for Plaintiff was compromised due to Equifax's acts and omissions and their failure to properly protect the PII.

5. Equifax could have prevented this Data Breach. Data breaches at other companies, including one of its major competitors, Experian have occurred.

6. The Data Breach was the inevitable result of Equifax's inadequate approach to data security and the protection of the PII that it collected during the course of its business.

7. Equifax disregarded the rights of Plaintiff by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard PII, failing to take available steps to prevent and stop the breach from ever happening and failing to monitor and detect the breach on a timely basis.

8. As a result of the Equifax Data Breach, the PII of Plaintiff and others has been exposed to criminals for misuse. The injuries suffered by Plaintiff or likely to be suffered by Plaintiff as a direct result of the Equifax Data Breach include:

a. unauthorized use of his PII;

b. theft of Plaintiff's personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of his financial accounts;

d. damages arising from the inability to use his PII;

e. loss of use of and access to his account funds and costs associated with inability to obtain money from his accounts or being limited in the amount of money he would be permitted to obtain from his accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on his credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity on the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identify theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being laced in the hands of criminals

and already misused via the sale of Plaintiffs' information on the Internet black market;

h. damages to and diminution in value of their PII entrusted to Equifax for the sole purpose of purchasing products and services from Equifax; and

i. the loss of Plaintiff's privacy.

9. The injury to Plaintiff was directly and proximately caused by Equifax's failure to implement or maintain adequate data security measures for PII.

10. Further, Plaintiff retains a significant interest in ensuring that his PII, which, while stolen, remains in the possession of Equifax is protected from further breaches, and seeks to remedy the harm he has suffered to him by his PII being stolen as a result of the Equifax Data Breach.

11. Plaintiff brings this action to remedy these harms on behalf of himself whose PII was accessed during the Data Breach. Plaintiff seeks the following remedies, among others statutory damages under the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(a)(1), in that this action involves parties of two different states.

13. This Court has personal jurisdiction over Equifax because Equifax maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Equifax intentionally availed itself of this jurisdiction by marketing

and selling products and services and by accepting and processing payments for those products and services within Georgia.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Equifax's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs claims occurred in the District.

PARTIES

15. Plaintiff Damian Flores is a resident of the State of Idaho, residing at 3666 Maryzell Lane, Pocatello, Idaho 83201. Plaintiff is a victim of the Data Breach.

16. Defendant Equifax Inc. is a Delaware Corporation with its principal place of business located at 1550 Peachtree Street NE Atlanta, Georgia 30309. Equifax Inc. may be served through its registered agent Shawn Baldwin, at its principle office address identified above, or its current counsel of record in these matters, David L. Balser, King and Spalding, LLP-ATL 40, 40th Fl., 1180 Peachtree Street NE, Atlanta, GA 30309-3521.

STATEMENT OF FACTS

17. Equifax is one of three nationwide credit-reporting companies that track and rate the financial history of U.S. consumers. The companies are supplied with data about loans, payments and credit cards, as well as information on everything from child support payments, credit limits, missed rent and utilities payments, addresses and employer history. All this information, and more factors into credit scores.

18. Unlike other data breaches, not all the people affected by the Equifax breach may be aware that they are customers of the company. Equifax gets its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records.

19. According to Equifax's report on September 7, 2017, the breach was discovered on July 29th. The perpetrators gained access by '[exploiting] a [...] website application vulnerability" on one of the company's U.S.-based servers. The hackers were then able to retrieve "certain files."

20. Included among those files was a treasure trove of personal data: names, dates of birth, Social Security numbers and addresses. In some cases -- Equifax states around 209,000 -- the records also included actual credit card numbers. Documentation about disputed charges was also leaked. Those documents contained additional personal information on around 182,000 Americans.

21. Personal data like this is a major score for cybercriminals who will likely look to capitalize on it by launching targeted phishing campaigns.

22. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII -- a form of intangible property that Plaintiffs entrusted to Equifax and that was compromised in and as a result of the Equifax Data Breach.

23. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

24. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their PII being placed in the hands of criminals who have already or will imminently, misuse such information.

25. Moreover, Plaintiff has a continuing interest in ensuring that their private information, which remains in the possession of Equifax, is protected and safeguarded from future breaches.

26. At all relevant times, Equifax was well-aware, or reasonably should have been aware, that PII collected, maintained and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

27. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, including Experian, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiff.

28. PII is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber black market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites, PII is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

29. Legitimate organizations and the criminal underground alike recognize the value in PII contained in merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches ... not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[1]

---

[1] Verizon 2014 PCI Compliance report, available at: http/www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereinafter "2014 Verizon Report"), at 54 (last visited November 25, 2017).

30. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if it data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

31. Equifax was, or should have been, fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals who would be harmed by a breach of Equifax's systems.

32. Unfortunately, and as alleged below, despite all this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Equifax's approach to maintaining the privacy and security of the PII of Plaintiff was lackadaisical, cavalier, reckless, or at the very least, negligent.

33. The ramifications of Equifax's failure to keep Plaintiff's data secure are severe.

34. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[3]

35. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have

---

[2] 17 C.F.R. § 248.201 (2013).
[3] *Id.*

personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[4]

36. Identity thieves can use personal information, such as that of Plaintiffs and Class members which Equifax failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

37. Javelin strategy and Research reports that identify thieves have stolen $112 billion in the past six years.[5]

38. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[6]

---

[4] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited November 25, 2017).

[5] See https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited November 25, 2017).

[6] Victims of Identity Theft, 2014 (Sept. 2015) available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited November 25, 2017).

39. There may be a time lag between when harm occurs versus when it is used. According to the U.S. Government Accountability Office ("GAO"), which, conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm of resulting from data breaches cannot necessarily rule out all future harm.[7]

40. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Plaintiff is incurring and will continue to incur such damages in addition to any fraudulent use of his PII.

41. The PII of Plaintiff is private and sensitive in nature and was left inadequately protected by Equifax. Equifax did not obtain Plaintiffs consent to disclose his PII to any other person as required by applicable law and industry standards.

42. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiffs PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs PII to protect against reasonably foreseeable threats to the security or integrity of such information.

---

[7] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited November 25, 2017).

43. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

44. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Equifax would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

45. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiff has been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting other financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's slippage, as is the case here.

46. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs PII, causing him to suffer, and continue to suffer, economic damages and other actual harm for which he is entitled to compensation, including:

a. theft of his personal and financial information;

b. unauthorized charges on his debit credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by his PII being placed in the hands of criminals and already misused via the sale of Plaintiffs information on the black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of his PII;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of his time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. ascertainable losses in the form of deprivation of the value of their PII and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. loss of use of and access to his account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

k. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate and deal with actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing

cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress nuisance and annoyance of the dealing with all such issues resulting from the Data Breach.

47. Equifax has not offered customers any meaningful credit monitoring or identity theft protection services, despite the fact that it is well known and acknowledged by the government that damage and fraud from a data breach can take years to occur. As a result, Plaintiff is left to his own actions to protect himself from the financial damage Equifax has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Equifax's actions have created for Plaintiff, is ascertainable and is a determination appropriate for the trier of fact. Equifax has also not offered to cover any of the damages sustained by Plaintiff.

48. While the PII of Plaintiff has been stolen, Equifax continues to hold PII consumers, including Plaintiff. Particularly because Equifax has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff has an undeniable interest in insuring that his PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CHOICE OF LAW

49. Georgia, which seeks to protect the rights and interests of Georgia and other U.S. residents against a company doing business in Georgia, has a greater interest in the claims of Plaintiff than any other state and is most intimately concerned with the claims and outcome of this litigation.

50. The principal place of business of Equifax, located at 1550 Peachtree Stet NE Atlanta, Georgia 30309, is the "nerve center" of its business activities - the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security, and where: a) major policy, b) advertising, c) distribution, d) accounts receivable departments and e) financial and legal decisions originate.

51. Furthermore, Equifax's response to, and corporate decisions surrounding such response to, the Data Breach were made from and in Georgia.

52. Equifax's breach of its duty to customers Plaintiff, emanated from Georgia.

53. Application of Georgia law to Plaintiffs claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiff.

54. Further, under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia will apply to the common law claims of Plaintiff.

COUNT I
NEGLIGENCE

55. Plaintiff restates and realleges Paragraphs 1 through 54 as if fully set forth herein.

56. Upon accepting and storing the PII of Plaintiff in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiff to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the PII was private and confidential and should be protected as private and confidential.

57. Equifax owed a duty of care to not subject Plaintiffs along, with their PII and to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

58. Equifax owed numerous duties to Plaintiff, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

59. Equifax also breached its duty to Plaintiff to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Equifax failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and, misuse the PII and intentionally disclose it to others without consent.

60. Equifax knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at Experian.

61. Equifax knew, or should have known, that data systems and networks did not adequately safeguard Plaintiffs PII.

62. Equifax breached its duties to Plaintiff by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiff.

63. Because Equifax knew that a breach of its system would damage millions of individuals, including Plaintiff, Equifax had a duty to adequately protect their data systems and

the PII contained thereon.

64. Equifax had a special relationship with Plaintiff. Plaintiffs willingness to entrust Equifax with his PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its systems and the PII it stored on them from attack.

65. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs PII. Equifax's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

66. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiff's Personal Information and promptly notify him about the data breach.

67. Equifax breached its duties to Plaintiff in numerous ways, including:

a. by failing to provide fair notice or adequate computer systems and data security practices to safeguard PII of Plaintiff;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs PII both before and after learning of the Data Breach;

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiffs PII had been improperly acquired or accessed.

68. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiff from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiff during the time it was within Equifax possession or control.

69. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the PII to Plaintiff so that Plaintiff can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of his PII.

70. Equifax breached its duty to notify Plaintiff of the unauthorized access by waiting many months after learning of the breach to notify Plaintiff and then by failing to provide Plaintiff information regarding the breech until September 2017. Instead, its executives disposed of at least $1.8 million worth of shares in the company after Equifax learned of the data breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiff regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff.

71. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiff from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiff during the time it was within Equifax's possession or control.

72. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiff from taking meaningful, proactive steps to secure their financial data and bank accounts.

73. Upon information and belief, Equifax improperly and inadequately safeguarded PII of Plaintiff in deviation of standard industry rules, regulations and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive PII of Plaintiff as described in this Complaint, created conditions conductive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiffs.

74. Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII, failing to conduct regular security audits, failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiff and failing to provide Plaintiff with timely and sufficient notice that his sensitive PII had been compromised.

75. Plaintiff never contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

76. As a direct and proximate cause of Equifax's conduct, Plaintiff suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiffs damages arising from Plaintiffs inability to use his debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as result of the Data Breach and/or false fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on his life including, inter alia, by placing "freezes" and "alerts" with credit

reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II
NEGLIGENCE PER SE

77. Plaintiff restates and realleges Paragraphs 1through 54 as if fully set forth herein.

78. Section 5 of the FTC Act prohibits "unfair ...practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

79. Equifax violated § 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiff.

80. Equifax's violation of § 5 of the FTC Act constitutes negligence per se.

81. Plaintiff is a person that the FTC Act was intended to protect.

82. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against

businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff.

83. As a direct and proximate result of Equifax's negligence per se, Plaintiff has suffered, and continue to suffer, injuries damages arising from Plaintiffs inability to use his debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees, charges and foregoing cash back rewards damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on his life including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT III
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA")

84. Plaintiff restates and realleges Paragraphs 1 through 54 as if fully set forth herein.

85. As Plaintiff is a consumer entitled to the protections of the FCRA 15 U.S.C. § 1681a(c).

86. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information non-consumers for the purpose of furnishing consumer reports to third parties...." 15 U.S.C. § 1681a(f).

87. Equifax is a consumer reporting agency under the FCRA because, for monetary

fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

88. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to...limit the furnishing of consumer reports to the purposes listed under § 1681b of this title." 15 U.S.C. § 1681e(a).

89. Under the FCRA, a "consumer report" is defined as "any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit...to be used primarily for personal family, or household purposes ...or (C) any other purpose authorized under § 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

90. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681B, "and other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed Plaintiffs PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

91. Equifax furnished the Plaintiffs consumer reports by disclosing Plaintiffs consumer report to unauthorized entities and computer hackers, allowing unauthorized entities and computer hackers to access their consumer reports knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing Plaintiffs consumer reports and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing his consumer reports.

92. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

93. Equifax willfully and/or recklessly violated §§ 1681b and 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under § 1681b of the FCRA. The willful ad reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breeches in the past. Further, Equifax touts itself as an industry leader in breech prevention thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

94. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.* 55 Fed. Reg 18804 (May 4, 1990), 1990 Commentary on The Fair Credit Reporting Act 16 C.F.R. Part 600, Appendix to Part 600, Sec. 607 2E. Equifax obtained

or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff of his rights under the FCRA.

95. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs personal information for no permissible purposes under the FCRA.

96. Plaintiff has been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiff is entitled to recover "any actual damages sustained by the consumer...or damages of not less than $100 and not more than $1,000." 15 U.S.C. §. 1681n(a)(1)(A).

97. Plaintiffs and the Nationwide Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) and (3).

COUNT IV
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

98. Plaintiff restates and realleges Paragraphs 1 through 54 as if fully set forth herein.

99. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under § 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming

to be an industry leader in data breach prevention. Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

100. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs PII and consumer reports for no permissible purposes under the FCRA.

101. Plaintiff has been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiff is entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

102. Plaintiff is entitled to recover his costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT V
DECLARATORY JUDGMENT

103. Plaintiff restates and realleges Paragraphs 1 through 54 as if fully set forth herein.

104. As previously alleged, Plaintiff entered into an implied contract that required Equifax to provide adequate security for the PII it collected from his payment card transactions. As previously alleged, Equifax owes duties to care to Plaintiff that requires it to adequately secure PII.

105. Equifax still possesses PII pertaining to Plaintiff.

106. Equifax has made no announcement or notification that is has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

107. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiff. In fact, now that Equifax's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

108. Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiff.

109. Plaintiff, therefore, seeks a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors

b. engaging third-party security auditors and internal personnel to run automated security monitoring

c. auditing, testing, and training its security personnel regarding any new or modified procedures

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services

f. conducting regular data base scanning and securing checks

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

COUNT VI
VIOLATION OF GEORGIA FAIR BUSINESS PRACTICES ACT ("GFBPA") O.C.G.A. § 10-1-390, *ET SEQ.*

110. Plaintiff restates and realleges Paragraphs 1 through 54 as if fully set forth herein.

111. Equifax is engaged in, and their acts and omissions affect, trade and commerce pursuant to O.C.G.A. § 10-1-392(28).

112. As discussed above, Equifax's acts, practices, and omissions at issue in this matter were directed and emanated from its headquarters in Georgia.

113. Plaintiff entrusted Equifax with his PII.

114. As alleged herein this Complaint, Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the GFBPA:

a. failure to maintain adequate computer systems and data security practices to safeguard PII

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft

c. failure to timely and accurately disclose the Data Breach to Plaintiff

d. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of PII and storage of other personal information after Equifax knew of should have known of the Data Breach and before it allegedly remediated the Breach.

115. Furthermore, as alleged above, Equifax's failure to secure consumers' PII violates the FTCA and therefore violates GFBPA.

116. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff, deter hackers, and detect a breach within a reasonable time, and that the risk of data breach was highly likely.

117. As a direct and proximate result of Equifax's violations of GFBPA. Plaintiff suffered damages including, but not limited to: damages arising from the unauthorized charges on his debit or credit cards or on cards that were fraudulently obtained through the use of Plaintiff's PII; damages arising from Plaintiffs inability to use his debit or credit cards or accounts because those cards or counts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and

detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

118. Also, as a direct result of Equifax's knowing violation of GFBPA, Plaintiff is entitled to damages as well as injunctive relief, including but not limited to:

a. Ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors

b. Ordering that Equifax engage third party security auditors and internal personnel to run automated security monitoring

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures

d. Ordering that Equifax segment PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems

e. Ordering that Equifax purge, and destroy in a reasonable secure manner PII not necessary for its provisions of services

f. Ordering that Equifax conduct regular database scanning and securing checks

g. Ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and

contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Equifax to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

119. Plaintiff brings this action on behalf of himself for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and the public form Equifax's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Equifax's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

120. Plaintiff is entitled to a judgment against EQUIFAX for actual and consequential damages, exemplary damages and attorney's fees pursuant to the GFBPA, costs, and such other further relief as the Court deems just and proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the court enter judgment in his favor and against EQUIFAX as follows:

a. Accept jurisdiction of this case;

b. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and /or disclosure of Plaintiffs PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff;

c. For equitable relief compelling Equifax to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Plaintiff the type of PII compromised;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' and paralegals' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

DATED 12/21/17

Respectfully submitted,

Damian Flores

Damian Flores
3666 Maryzell Lane
Pocatello, Idaho 83201
~~(208) 241-2819~~ 208-252-8987

VERIFICATION

I have read the foregoing Complaint and hereby verify that the matters alleged therein are true, except as to matters alleged on information and belief, and, as to those, I believe them to be true. I certify under penalty of perjury that the foregoing is true and correct. 28 U.S.C. § 1746.

Executed at

Respectfully submitted,

Damian Flores

Damian Flores
3666 Maryzell Lane
Pocatello, Idaho 83201
~~(208) 241-2819~~ 208-252-8987